

The Evolving Art of Networking Self-Defense

The network security paradigm is shifting. In the past, network security design could be said to resemble a fortress protected by concentric layers of defensive “walls.” But today’s security paradigm more closely resembles a living organism: a flexible outer layer of “skin” combined with a variety of internal immunity systems that extend protection down to individual “cells.”

In other words, networks are evolving toward greater internalization of the security function. In the process, they are learning to defend themselves from end to end—down to the endpoints that define the new network edge.

It’s not difficult to see the reason for this paradigm shift. Every networked device—from a PDA to a core router—can potentially be a point of attack. With the increase in both internal and external attacks comes the need for a network-based defense system that can encompass all these elements. The outward-facing defenses represented by firewalls are necessary, but not sufficient, to protect all the assets and resources residing throughout today’s networks.

The four primary business advantages to implementing a network-wide security system are:

- **Availability.** A fully protected network helps immunize the enterprise against lost productivity caused by disruptions.
- **Integration.** Holistic security systems can take advantage of the security components that have been imbedded in a variety of devices and software, extending all the way to endpoints such as PCs, application servers, and PDAs.
- **Automation.** The network can be instrumented to implement policies and accomplish security tasks with minimal intervention, lowering administrative overhead.

- **Responsiveness.** Changes in security policies can be made quickly, from a central location, and disseminated throughout the network.

Together, these advantages can add up to significant cost savings for enterprises of any size.

A Holistic Approach

As it makes further inroads into network infrastructure and aligns more closely with business processes, network security has moved beyond traditional perimeter defenses into the more inclusive, holistic area of systems management. For instance, patch management has been transformed from a reactive overlay process into an adaptive feature integrated into access control and posture assessment.

To substantially improve network security, IT needs to focus not just on firewalls (at the perimeter and elsewhere), but also on the individual hosts, the network connectivity devices, and the various software agents that provide communication and control functions. All these components should come under the auspices of a comprehensive set of security policies that are firmly tied to business requirements and based on accurate posture and vulnerability studies.

For a system-level security solution to perform effectively, the information that is exchanged by the various subsystems must be trustworthy. That trust should begin with session initiation and continue until session termination. For instance, devices should be able to examine the interaction between, say, a client and server, to make sure one of them hasn't been compromised and has begun launching attacks on the other. This holistic approach emphasizes the interrelations among the network elements as well as the intervention capabilities that discover and mitigate threats.

Defending the Hosts

Traditionally, host systems have been protected by reactive technologies such as antivirus software and operating system patch management. This level of security, combined with

perimeter firewalls and physical security measures, was thought to be sufficient to thwart most attacks involving endpoint

Today, however, many users take their computers with them when they leave the office and link them to the network from home or while traveling. This opens new avenues for malware and other threats to enter the enterprise network. For example, spyware could potentially grab a user's password when the user connects to the corporate network through a public hotspot. The password could subsequently find its way into a hacker assault. Or a Trojan horse that might normally be caught by enterprise perimeter firewalls could sneak onto a laptop during a download at home and infect the network when the computer is plugged in back at the office. While technologies such as virtual private networks (VPNs) can help secure remote connections, they don't address these other types of threats.

In addition, hosts may be rendered vulnerable to attacks because they've missed out on the latest patch, or haven't received it in time. Patch management products can speed this process. Still, patching is a process that by its very nature can't offer "day-zero" protection against new exploits that haven't even been identified yet.

Servers don't ordinarily leave the premises, but like desktop devices they are vulnerable to internal attacks emanating from other devices sitting behind the enterprise firewall and from exploits masquerading as legitimate traffic coming from the outside. Servers performing critical functions or containing valuable data can be walled off by internal firewalls or virtual LANs that permit access only to trusted individuals or specific groups. But these remedies do nothing to ferret out and neutralize any successful intrusions that do occur, and they can be circumvented by a relatively simple, internally based attack.

Additional Host Protection

Host protection can be augmented by three additional measures: behavior-based blocking, posture assessment, and network admission control.

Behavior-based blocking technology protects the endpoints by looking for out-of-policy behavior or attempted attacks in processes associated with applications or services, enabling the technology to block the exploits proactively before they can disrupt critical operations. Endpoint security agents provide this protection by comparing system calls, application-oriented events, and other activities to a set of behavioral rules that have been established according to expected relationships or “correlations,” then dynamically applying these rules. Because specific exploit signatures are not required, this method can protect the host regardless of its patch or antivirus levels.

A posture assessment is an evaluation of the current security state of the entire network. The host portion of an internal posture assessment should include activities such as examining port vulnerabilities and trust relationships between hosts, as well as determining how well host configurations and defenses conform to security policies. With an accurate and detailed posture assessment in place, IT can apply the appropriate access rights and correct host deficiencies in a timely manner.

Network admission control is gate-keeping technology that uses the intelligence embedded in the network infrastructure to enforce security policy on noncompliant endpoints before they are connected and able to access network resources. Hosts that meet the security criteria gain entry quickly, while those that aren’t compliant are either denied a connection or quarantined in a protected segment for further attention.

Network admission control systems work through agents residing on each host that query security software and communicate status to a policy server, where that status is compared against a set of policies established by IT and enterprise management. The system must be flexible enough to operate with all the other internal security solutions that have been deployed across the network—including antivirus software, internal firewalls, intrusion detection measures, patch management products, and the host operating system—regardless of vendor. For this reason, industry standards and partnerships will be critical to the success of any admission control initiative.

What's more, the network admission control system needs to provide extensive coverage of all the access methods that hosts use to connect with each other—wired LAN, wireless LAN (WLAN), WAN, and remote connections. This is where network access devices come into play. Routers, switches, VPN access concentrators, firewalls, and other devices can be authorized to assign credentials to endpoints, and demand that those credentials be presented and verified whenever the endpoint initiates a network connection.

Securing Other Network Elements

In addition to host defense, IT needs to pay close attention to securing critical routing and switching devices. Overall security may also be increased by extending protection to specific enterprise-critical applications such as voice over IP (VoIP), and to potentially vulnerable elements such as wireless access points.

Routers and switches must be equipped with functions that enable these devices to defend themselves, and also to prevent attacks on servers. As an example, a behavior-based tool called anomaly detection can detect and report on distributed denial of service (DDoS) attacks, worms, and other exploits by comparing actual network activity to historically normal behavior. Suspicious traffic is then diverted from the target server before it can cause an overload or otherwise disrupt operations. Anomaly detection may be combined with an intrusion prevention system (IPS) that looks deeper into packet payloads to provide even broader protection against viruses, worms, and spyware.

IP telephony, call-control applications, Web-enabled services, and other types of network applications represent yet another layer of resources that needs to be shielded from threats. This application protection can be accomplished with a combination of policy-enforcing firewalls, router-based inspection and control to guard against port-80 misuse, and sophisticated VPNs with application-protection capabilities.

On the wireless front, WLANs need to be integrated more fully with the rest of the security infrastructure. Security capabilities in wireless switches and other devices will

help accomplish this goal. Distributed security intelligence also can aid in identifying rogue access points that can be hard for intrusion-detection software to spot.

Encryption Everywhere

The anytime, anywhere nature of network access demands anytime, anywhere security. And in part that means pervasive encryption. To prevent data, voice, and video packets from being read or altered by intruders, they must be encrypted wherever they are vulnerable to compromise.

Enterprise wireless communications, which are essentially radio broadcasts, should always be strongly encrypted. Without hard-to-crack encryption technology, it's possible for a hacker to not only listen in on a transmission, but also to alter or corrupt the data and retransmit it without ever establishing legitimate network access.

Router-to-router encryption across the LAN and WAN is also an important precaution for any enterprise that wants to avoid eavesdropping or data tampering on communications that are sent between secure networks. VPN encryption helps safeguard remote connections in many enterprises. However, many suppliers, resellers, and other partner organizations must cooperate to make sure that encryption and other security measures have been adequately deployed and security policies have been coordinated all the way across enterprise-to-enterprise extranets.

In the future, encryption will be implemented on a spectrum of network devices, providing the ability to encrypt traffic at all levels and across all nodes. Internal encryption not only thwarts data theft, it also helps prevent hijacking, tampering, and other activities that interfere with network communications. With enterprises increasingly relying on converged IP networks to carry the entire communications load—including all the data, voice, and video traffic—shielding those interconnected services from harm has become a paramount concern.

Encryption presents problems for security solutions because these products must be able to decrypt the traffic in order to examine it and apply the appropriate security procedures. Case in point: an encrypted worm could get past a firewall or intrusion detection appliance that can't look closely enough at the incoming packets. For this reason, decryption capabilities will need to be built in to the security solutions in such a way that traffic isn't delayed.

Summing Up

In today's multilevel threat environment, network security is looking less like a medieval castle and more like a highly evolved organism. Because many attacks simply can't be discovered or stopped at the traditional network edge, enterprises need to adopt a holistic, end-to-end approach to securing network-attached resources. That means a strong security presence in a multitude of network devices—most definitely including the endpoints.

Many of the solutions described above will demand a level of network intelligence and cross-communication that can only be achieved through strong partnerships among network security vendors. These associations are already in progress, and auger well for the future.